AHMAD KHALIL, S. ANANDHA KRISHNA RAJ

Development and Deployment of Autonomous Weapon Systems: Comprehensive Analysis of International Humanitarian Law

Abstract

This paper addresses the problem of the need to determine the legality of autonomous weapon systems (AWS) under international human law (IHL), focusing on the two targeting and weapons laws. This study emphasizes the need not to confuse these two laws in the analysis. The paper aims to clarify whether AWS could be considered illegal under IHL, taking into account the principles of distinction, proportionality and precaution. The research methodology includes an analysis of the relevant provisions of IHL and customary humanitarian law. The research design includes an examination of the potential of AWS to cause unnecessary injury or suffering and their classification as indiscriminate weapons. The paper concludes that while AWS possess autonomous decision-making capabilities, human oversight is required to prevent excessive harm.

KEYWORDS: Autonomous Weapon Systems, Artificial Intelligence, International Humanitarian Law, Weapons Law, Targeting Law, Martens Clause

AHMAD KHALIL, PhD candidate at VIT School of Law, VIT University, Chennai, Tamil Nadu, India, ORCID – 0009-0007-0615-9812, e-mail: ahmadkhalil5665@gmail.com
S. ANANDHA KRISHNA RAJ, Associate Professor at VIT School of Law, VIT University, Chennai, Tamil Nadu, India, ORCID – 0009-0001-0177-1689, e-mail: anandha.krishnaraj@vit.ac.in

HTTPS://DOI.ORG/10.36128/PRIW.VI50.774

1 Introduction

New tactics, the shifting global geopolitical landscape, and technological advances are challenging preconceived notions of combat and its changing nature. Although not always welcome, a legal debate is required to control new combat technologies. Due to the extreme complexity of the technological infrastructure of AWS, it has been said that lawyers have limited relevant input to make[1]. Roboticists are the vanguard of a third wave of weaponry that fundamentally changes the dynamics of warfare[2]. Throughout history, however, the legal framework has remained central to the integration of new technologies during previous military transformations. Rather than hindering progress, its role has ensured the preservation of universal humanitarian principles enshrined in international humanitarian law and global legal norms.

The technology utilized in warfare is inherently influenced by human design and programming, rendering it incapable of being truly „unbiased". Therefore, it must be steadily dedicated to upholding well-established international principles. Primarily, the focus is on safeguarding these standard values, which prompts thorough consideration of deploying emerging technologies. This includes assessing the need for protective protocols, determining human involvement in machine interfaces, and, most importantly, ensuring accountability for inevitable errors and violations that occur in combat situations[3]. In addition, the ability to program artificial intelligence (AI) to discriminate, adapt, take precautions, and consist of procedures that are already complex for a human fighter will be discussed.

Opinions on the legitimacy of AWS are divided into two opinions. Supporters focus on the advantages of precision, which ensures better distinction and proportionality[4]. The other party that opposes the AWS

1 Henderson Ian, Patrick Keane, Joshua Liddy, „Remote and Autonomous Warfare Systems – Precautions in Attack and Individual Accountability", [in:] *Research Handbook on Remote Warfare*, ed. Jens David Ohlin (Cheltenham: Edward Elgar Press, 2016), 24.

2 Christopher Coker, „On Banning Autonomous Weapon Systems: Human Rights, Automation and the Dehumanization of Lethal Decision Making" *Future Wars*, (2015): 57-60.

3 Ahmad Khalil, S. Anandha Krishna Raj, „Deployment of Autonomous Weapon Systems in the Warfare: Addressing Accountability Gaps and Reformulating International Criminal Law" *Balkan Social Science Review* 23, No. 23 (2024): 261-285.

4 Crootof Rebecca, „The Killer Robots Are Here: Legal and Policy Implications" *Cardozo Law Review*, No. 5 (2015): 1837-1916.

claims that it is necessary to ban them, especially because of the problems of discrimination and proportionality, which are impossible to measure and program[5]. The real difficulty in adhering to these principles lies in the fact that they will sometimes be in complex environments, such as using AWS in urban warfare[6].

While military experts believe that AWS ability exceeds the ability of humans to work in certain contexts, this would constitute an advantage. In addition to the fact that the development of AWS is of military importance, they can also be an effective tools on the economic level.

IHL rules always seek to limit the methods and means of warfare, both in and outside times of armed conflict. This would guarantee protection for individuals, preserve their human dignity, and respect the rights of civilians and other legally protected groups. Using AWS raises relevant legal and ethical questions regarding guarantees that the regime complies with the standards of IHL when selecting and attacking targets.

Since the beginning of discussions on AWS, scholars have researched the legality of AWS in their literature. This prompted this comprehensive analysis of the legality of AWS based on the basic pillars of IHL. Acknowledging that no legal instruments regulate AWS, particularly, does not negate its subjection to weapon law rules. The general principles on which weapons law is based govern the right to ban weapons. Normative principles are first evident in the fact that the weapon is, by its nature, not indiscriminate or causes superfluous injury or unnecessary suffering. Ensure that they are directed only at military targets to protect civilians and their objects by distinguishing them from combatants[7]. As for the use stage in combat, the weapon must be subject to the rules of the organization of hostilities or targeting law.

5 Lucy Suchman, „Algorithmic Warfare and the Reinvention of Accuracy" *Critical Studies on Security*, No. 2 (2020): 175-187. https://doi.org/10.1080/21624887.2020.1760587.

6 Peter Asaro, „Jus Nascendi. Robotic Weapons and the Martens Clause", [in:] *Robot Law*, ed. Michael A. Froomkin, Ryan Calo, Ian Kerr, Edward Elgar (Cheltenham, 2016), 367-386. https://doi.org/10.4337/9781783476732.00024.

7 Anderson Kenneth, Reisner Daniel, Waxman Matthew C., „Adapting the Law of Armed Conflict to Autonomous Weapon Systems" *International Law Studies*, (2014): 386-411.

2 The Concept of Autonomy in Weapon Systems

Most definitions in the legal field often revolve around the idea that the word refers to a weapon system that is capable of selecting and engaging a target without the need for human intervention. Considering the importance of this definitional method, it is helpful to understand its components. A weapon is any device designed to harm, destroy, or hurt people or property[8]. Furthermore, there is no differentiation made between weapons intended to cause death or injury.

As for selecting and engaging a target, most people infer „select" as „choose among" a gathering or group[9]. Moreover, it is important to define „engage" in the military sense, which usually means fight[10]. „Engage" concerning AWS might mean at least three distinct things at various times: activation stage, operation stage, and use of force stage (killing decision), it is important to understand the last position better[11]. Therefore, using this method, the machine system selects a certain target and decides when and where to use the weapon to engage it.

The last part of the definition stipulates that the system must take operate „without human intervention"[12]. It is not always evident whether humans are involved in a weapons system and, if so, to which level. The ICRC has observed that both automaticity and autonomy are systems that can choose and attack targets independently while remaining within the stipulations of their human-determined programming. Making the distinction between the two somewhat blurry[13]. This raises the question of what level of system independence is needed for the system to be thought of as functioning without human intervention.

---

8 Taddeo Mariarosaria, Alexander Blanchard, „A Comparative Analysis of the Definitions of Autonomous Weapons", [in:] *The 2022 Yearbook of the Digital Governance Research Group* (Cham: Springer Nature Switzerland, 2023), 57-79.

9 Paul Scharre, Michael C. Horowitz, „Autonomy in Weapon Systems" *Center for a New American Security Working Paper*, (2015).

10 Stephen Morillo, *What is Military History?* (Hoboken: John Wiley & Sons, 2017).

11 Ankita Surabhi, *From „Killer Robots" to Autonomous Weapons Systems (AWS)*, 2019.

12 Joel M. Haight, Vladislav Kecojevic, „Automation vs. human intervention: What is the best fit for the best performance?" *Process Safety Progress*, No. 1 (2005): 45-51.

13 „Expert Meeting: Autonomous Weapon System: Technological, Military, Legal, and Humanitarian Aspects" ICRC, (2014), 5.

The ICRC distinguished between automatic and autonomous systems in the degrees of freedom in choosing and attacking targets[14]. While some believe that the difference between automated and autonomous systems is the ability to predict them according to the environment in which they operate. The main criterion is the organized environment in which the autonomous system is operated[15]. Nevertheless, this criterion is inaccurate because AWS may be deployed in organized environments, and automated systems may be operated in organized environments.

Since prediction is a controversial matter, others believe that it is possible at the level of generality and not specificity. Predicting the destruction of a specific military target is a general and predictable task. As for the specific ones, they are the precise procedures upon which the system operates and cannot be predicted. Therefore, according to their claim, the basic criterion for distinguishing between an automated and an autonomous system is the predictability of its working procedures[16].

It becomes clear that distinction between the two systems is a complex matter, stemming from the simplicity of the approach followed by the definition. Regardless of the disagreement, leaving the decision to a machine to decide to kill by itself is morally and legally unacceptable, so this matter must be researched, especially from the perspective of IHL. But before the legal analysis, we must explore the stage of the development of the autonomy which have reached to it in the weapon systems at the present time.

3 The Current State of AWS Development

The United States (US) is at the forefront of technologically advanced countries, developing naval weapons systems (surface and subsurface) and unmanned aerial systems for various purposes. For example, as a result of cooperation between the US Department of Defense (DOD) and the

14 Nurbanu Hayir, „Defining Weapon Systems with Autonomy: The Critical Functions in Theory and Practice" *Groningen Journal of International Law*, No. 2 (2022): 9.

15 Christof Heyns, „Extrajudicial, Summary or Arbitrary Executions" *Security Issues in the Greater Middle East*, (2013): 183.

16 Christopher M. Ford, „Autonomous Weapons and International Law" *South Carolina Law Review*, 69 (2017): 413.

Massachusetts Institute of Technology (MIT), they worked on the development of autonomous air weapon systems with the swarming features[17]. The swarming feature is formed from the initial launch of small-sized kamikaze drones[18]. These kamikazes are considered unmanned aerial systems that contain a warhead and are equipped with sensors to understand the surroundings, identify the target, and cause an explosion when it hits the target[19].

Other nations are developing these weapon systems in addition to the US. The nEUROn military system, which has been under development since 2016, is considered the most advanced and characterized by its longevity. The system belongs to the Intelligence, Surveillance, and Reconnaissance (ISR) systems manufactured by Dassault Aviation of France[20]. Furthermore, British Aerospace focuses on developing the Taranis autonomous UAV. Simultaneously, Israel has developed an autonomous UAV called „Harpy", and it also has an autonomous underwater anti-mine weapon called „Seagull" that is designed to carry out missions against both individual divers and submarines. In application, for example, South Korea deployed the Sentry Guard Robot-1 (SGR-1) to carry out the task of protecting the Korean Demilitarized Zone.

In 2017, the Turkish Kargu-2 autonomous attack drone was manufactured by STM (Savunma Teknolojileri Mühendislik ve Ticaret A.)[21]. Furthermore, according to the UN Report 2021, an STM Kargu with explosives was discovered and attacked Haftar's soldiers in Libya in 2020.[22]

17 Michael Hardy, „Pentagon Proves Air-Launched UAV Swarm Ability" *C4ISRNet*, 19 August 2022. https://www.c4isrnet.com/unmanned/uas/2016/03/15/pentagon-proves-air-launched-uav-swarm-ability/. [accessed: 2.05.2023].

18 Bitar Mohammad, Chakka Benarji, „Drone Attacks During Armed Conflict: Quest for Legality and Regulation" *International Journal of Intellectual Property Management*, No. ¾ (2023): 97-411.

19 James Drew, „USAF's Small UAS Roadmap Calls for Swarming «kamikaze» Drones" *Flight Global*, 10 December 2019. https://www.flightglobal.com/civil-uavs/usafs-small-uas-roadmap-calls-for-swarming-kamikaze-drones/120493.article. [accessed: 4.05.2023].

20 „Neuron Unmanned Combat Air Vehicle (UCAV) Demonstrator" *Airforce* Technology, 18 February 2020. https://www.airforce-technology.com/projects/neuron/. [accessed: 6.05.2023].

21 „STM Kargu" *Smartencyclopedia*, 4 January 2023. https://smartencyclopedia.org/content/stm-kargu/. [accessed: 6.05.2023].

22 Joe Hernandez, „A Military Drone with a Mind of Its Own Was Used in Combat, U.N. Says" *NPR*, 1 June 2021. https://www.npr.org/2021/06/01/1002196245/a-u-n-report-suggests-libya-saw-the-first-battlefield-killing-by-an-autonomous-d. [accessed: 8.05.2023].

Also, according to media reports, in 2020, „Kamikaze" and „Kargu-2" were deployed in Nagorno-Karabakh during the Armenia-Azerbaijan war[23].

Contrary to the claims of HRW and opponents of the AWS ban, some believe that machines will never be able to judge emotion and intent. Technology has already demonstrated a growing capacity to read multiple facial recognition patterns more accurately. In isolation from direct physical contact, it can also determine the rate of stress using digital cameras „sensory"[24]. Similar technologies, „sensory", are utilized to determine mental states like satisfaction and desperation in human behavior patterns[25].

Several scholars have created methods for measuring and identifying human emotions using wireless signals and computer learning; hence, the system then uses machine learning, the „emotion classifier", to determine a person's mood without making physical touch[26]. Some legal experts contend that robots that detect human emotions are not a precondition for their lawful employment. Instead, they argue that it is feasible to design a set of control procedures that are readily accepted and implemented to guarantee that countries can use LAWS according to international law. A proper algorithm, in conjunction with and carried out by a correctly created system[27], may generate a set of precautionary employment TTPs to guarantee that the militaries can use LAWS under the IHL. Therefore, you will move on to the comprehensive legal analysis of AWS from the perspective of weapons law and targeting law.

---

23 Robin Forestier-Walker, „Nagorno-Karabakh: New Weapons for an Old Conflict Spell Danger" *Al Jazeera*, 13 October 2020. https://www.aljazeera.com/features/2020/10/13/nagorno-karabakh-new-weapons-for-an-old-conflict-spell-danger.

24 Daniel J. McDuff, Javier Hernandez, Sarah Gontarek, Rosalind W. Picard, „Cogcam" *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, No. 3 (2016): 4000–4004. https://doi.org/10.1145/2858036.2858247.

25 Asaph Azaria, Asma Ghandeharioun, Akane Sano, Rosalind Picard, Natasha Jaques, Sara Taylor, *Predicting Students' Happiness from Physiology, Phone, Mobility, and Behavioral Data*. International Conference on Affective Computing and Intelligent Interaction and workshops: [proceedings]. ACII (Conference), September 2015. https://pubmed.ncbi.nlm.nih.gov/28515966/.

26 Charles Q. Choi, „Mood-Detecting Sensor Could Help Machines Respond to Emotions" *IEEE Spectrum*, 24 June 24 2021. https://spectrum.ieee.org/mooddetecting-sensor-could-help-machines-respond-to-emotions.

27 Dustin A. Lewis, „Three Pathways to Secure Greater Respect for International Law Concerning War Algorithms" *Harvard Law School.PILAC* (2020). https://pilac.law.harvard.edu/three-pathways-to-secure-greater-respect-for-international-law-concerning-war-algorithms.

4 Legal examination of AWS's Development and Deployment

Undoubtedly, the current autonomy approach in AI represents greater complexity than before, as the AWS outputs are not necessarily subject to the same rules they were programmed to, although the programming greatly limits their self-decision[28]. For example, Slaughterbots, an autonomous aerial vehicle, can find and follow targets. Its system processes personal data, including images and information, on social media sites to identify and attack targets. The behaviour here is very complex, explaining to us what we referred to through pre-programming and its intertwining with independence, which explains the depth of complexity involved in understanding AWS.

Indeed, any use of any new weapon or method of warfare, such as AWS, must be subject to IHL. At a stage before use, the new weapon must be reviewed to ensure its compatibility with IHL. As for the use stage in combat, the new weapon must be subject to the rules of the organization of hostilities.

Thus, „weapons" and „means of warfare" refer to the initial question, „Is the weapon itself lawful?", while „methods of warfare" refer to the subsequent question, „Is the manner in which the weapon is used lawful?". Therefore, two aspects must be studied to provide a clear picture of the legitimacy of AWS. First, the weapons law, and second, the targeting law.

4.1. Weapons law

The IHL is considered a law that evaluates the legality of any weapon. Moreover, IHL specifies weapons prohibited in specific instruments, while those not specifically mentioned are subject to its evaluation rules. The mere use of weapons prohibited by specific instruments is a crime without regard to the consequences. Can AWS be considered illegal in itself without the need for additional legal rules under IHL?

28 Jutta Weber, Lucy Suchman, „Human–Machine Autonomies", [in:] *Autonomous Weapons Systems: Law, Ethics, Policy*, ed. Nehal Bhuta, Susanne Beck, Robin Geiβ, Hin-Yan Liu, Claus Kreβ (Cambridge: Cambridge University Press, 2016), 75-102.

Therefore, some argue that the difficulty of predicting the results of AWS makes it difficult to accept the idea of a ban before using them[29]. This is because the application of the principles can only be on a weapon in use. Therefore, it is important to research IHL rules, whether in treaties or international customary law, to determine the legality of AWS. This paper will subject AWS to the general principles of weapons law regulating means of warfare in the light of no specific instrument prohibiting them. To ascertain whether AWS would be deemed illegal under IHL. We will begin by clarifying the IHL's considerations regarding the legality of weapons.

Article 35 of API stated that „The right of the Parties to the conflict to choose methods or means of warfare is not unlimited". Furthermore, the second para of the same article also confirms that „It is prohibited to employ weapons, projects and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering".

Some argue that most of the weapons banned under specific instruments were due to the risk posed by their use[30]. The gap relating to human decision in the stage of using the final force of deciding to kill in AWS threatens the attribution of the responsibility process in its traditional sense under the pretext of the lack of human control, judgment, or participation. Article 36 of the API states that human beings must control decisions to kill or the final-stage decision to use force.

The complexity of applying IHL rules of distinction, proportionality, and precautions results from the unpredictability of AWS outcomes in operational environments. It sheds light on a critical feature of gun law. These rules are intended to protect permissible targets that is, military objectives that is, combatants in the first place.

In a landmark Advisory Opinion issued in the Nuclear Weapons case, ICJ established the two fundamental principles that form the core of IHL[31]. The first principle, rooted in the principle of discrimination, encompasses the prohibition against directly targeting civilians and civilian objects. Additionally, it encompasses the ban on using indiscriminate weapons, defined as those incapables of distinguishing between civilian and military targets. The second principle prohibits the use of weapons that cause

29 Maciej Zając, „Beyond Deadlock: Low Hanging Fruit and Strict yet Achievable Options in AWS Regulation" *Journal of Ethics and Emerging Technologies*, No. 2 (2022): 1-14.

30 David Turns, „Weapons in the ICRC Study on Customary International Humanitarian Law" *Journal of Conflict & Security Law*, No. 2 (2006): 201, 204.

31 Nuclear weapons Advisory Opinion; Greenwood (n 4) 445-446.

unnecessary suffering to legitimate targets or unnecessarily exacerbate their suffering. This is also called the „SIrUS rule" by the ICRC, which specifies that weapons should not cause harm greater than unavoidable to achieve legitimate military objectives[32]. Furthermore, a general rule regarding the development and deployment of weapons obliges states to conduct a legal review of the weapon in question, as stipulated in Article 36 of API.

4.1.1. AWS and Causing of Superfluous Injury or Unnecessary Suffering

Weapons that cause (*maux superflus*) are prohibited under both Article 35(2) API and Article 24(e) of the Hague Conventions IV. This rule has become customary over time and is present in most treaties dealing with weapons law.

Before any analytical application of the principles can be made, it must be made clear that AWS are not like other weapons. The fundamental difference between conventional weapons and AWS are the independent nature of performance, especially in the targeting decision. Moreover, the concept of AWS are to delegate the decision to use a weapon to a system that runs on AI. The difference is clear in terms of the impact and the damage that could be caused by using weapons to delegating the use of weapons to an autonomous system. From this standpoint, it cannot be said that AWS will inevitably cause certain suffering. Moreover, the notion that AWS may cause superfluous injury or unnecessary suffering cannot be accepted in all circumstances, if we take into account that AWS are a system in general.

Upon closer examination, it became clear that independence itself cannot have a direct negative consequence on the effects of use (harmful effects). Of course, there are weapons themselves that have direct effects by causing injury and suffering, therefore, questions arise about fully equipping the regime with such weapons or ammunition. The logical answer is to ban every weapon system that is equipped with munitions or weapons that, by their nature, cause superfluous injury or unnecessary suffering. AWS are not always classified as a system. When AWS are used as a weapon, this is exclusively when we want to differentiate between AWS as a system equipped with weapons or as a weapon itself[33]. It considers the possibility of the system causing acts that lead to excessive injury or

32 Robin M. Coupland, „Review of the Legality of Weapons: a New Approach" *International Review of the Red Cross*, No. 835 (1999): 583.

33 Liu Hin Yan, „Categorization and Legality of Autonomous and Remote Weapons Systems" *International Review of the Red Cross*, No. 886 (2012): 94.

unnecessary suffering if it is programmed to commit these acts. In this case, it is excluded to consider the type of ammunition or weapon with which the system is equipped. Such a scenario is unlikely and will not be subject to comparison for every AWS as a weapon system. However, the impact of the legal evaluation will only be on that particular case. Therefore, the legal assessment of AWS as a whole will not be affected. The aforementioned possibilities do not suffice to consider AWS as a whole unlawful in terms of causing unnecessary suffering or excessive injury. AWSs that may be considered in conflict with this principle are subject to specific scenarios that do not apply to the entire category. Therefore, the autonomy feature of AWS does not, in and of itself, cause excess injury or needless suffering.

Ultimately, the level of human oversight required over crucial functions must be adequate to guarantee that the harm from using the AWS does not surpass the anticipated military benefit. The assessment of this requirement relies on the type of ammunition utilized by the weapon system in question; thus, the fact that the actual deployment of force is orchestrated through an AI-driven process does not seem to be the determining factor.

4.1.2. AWS and the Indiscriminate Weapons

Regarding the potential targeting of a military objective by an AWS, as mandated by Article 51(4)(b) of the API, it is necessary to clarify that the present technology forming the foundation of the AWS, along with anticipate technological advancements, indicates that current or near-future systems are improbable to distinguish in situations involving anti-personnel application of force effectively[34].

Nevertheless, it would be unreasonable to overlook the potential for future advancements in the capacity of AI to distinguish between various types of objects. In addition, the development and deployment of indiscriminate AWS appear improbable, given their limited military utility[35]. Furthermore, beyond applications involving anti-personnel measures, operational systems could be considered predecessors to AWS or basic

34 Nils Melzer, *Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare*, (Directorate-General for External Policies, European Parliament, 2013), 28.

35 Christopher Toscano, „«Friends of Humans»: An Argument for Developing Autonomous Weapons Systems" *Journal of National Security Law & Policy*, No. 1 (2015): 189, 206.

versions of AWS[36]. These systems can distinguish between various signs, exemplified by some of the antiarmor missiles' capacity to discern between different vehicle types[37]. It has been argued that with the advancement of new technologies, AWS can exceed the current human capacities to uphold the distinction principle[38]. Whether this assertion materializes depends on the trajectory of technological development and the specific technology integrated into the AWS. The configuration of an AWS, particularly concerning sensor technology and system intelligence, will significantly influence its capacity for distinction, as autonomy alone does not always guarantee this capability.

Nevertheless, the scenario where an AWS are unable to distinguish between civilians and combatants does not inevitably preclude its potential to be directed at a military objective under any circumstances. There remains the possibility that such AWS could still be utilized if measures are taken to minimize the possibility of encountering non-combats during their deployment. Such mitigation may include restricting their use to certain environments[39].

An alternative approach to implementing such precautions involves setting specific task parameters, such as selecting the operational area or regulating the degree of force employed by the AWS. In this aspect, AWS can be likened to indiscriminate weapons, as they may produce indiscriminate outputs but are not in every scenario; their impact depends on the context of their deployment. Adhering to these precautions would enable the deployment of AWS while upholding the distinction principle, even if they lack this capability. It should be noted that AWS could be used in a discriminatory manner by programming specific legitimate goals for the system to achieve, effectively directing its focus to those goals.

When examining the issue of unmanageable outputs, as stipulated in Article 51(4)(c) of the API, there seems to be nothing inherent in the autonomy of the killing decision that could be debated to result in unsupervised outputs as envisioned by this provision. It is essential to distinguish

36 Rebecca Crootof, „The Killer Robots Are Here: Legal and Policy Implications" *Cardozo Law Review*, No. 36 (2015): 1837, 1842-1843.

37 Brian Handy, *Royal Air Force Aircraft & Weapons (DCC(RAF)* (Publications Belmont Press, 2007), 87; Crootof, „The Killer Robots Are Here", 1870-1871.

38 Shane Reeves, William Johnson, „Autonomous Weapons: Are You Sure These Are Killer Robots? Can We Talk About It?" *The Army Lawyer*, (2014): 25, 26.

39 George R. Lucas Jr, „Automated Warfare" *Stanford Law & Policy Review*, 25 (2014): 317.

between unmanageable outputs stemming from an AWS and the common direction that an AWS should be categorized as unmanageable. The notion of unmanageability concerning AWS differs from what is under Article 51(4)(c) of API. When discussing AWS, unmanageability refers to the inability of someone to directly control the actions of the system once it has been deployed. Typically, autonomy in this context refers to the precise actions of a system that are unsupervised.

This implies that the unmanageability of AWS does not suggest that the system is prone to indiscriminately targeting both combatants and civilians, as it can only operate within the limits of its programming and functioning standards and, in many instances, can likely be deactivated[40]. Therefore, unless AWS are equipped with a weapon that produces unmanageable outputs, such as prohibited weapons, it does not appear that an AWS would entail unmanageable outputs[41].

One could argue that Cyber Attacks could be entirely unsupervised, as evidence suggests that the spread of infection by these attacks cannot always be managed as presented by Article 51(4)(c) of the API[42]. A notable instance of such a scenario was the Stuxnet worm, which spread unsupervised and indiscriminately. However, this example demonstrates that payload delivery was controlled despite the worm's unsupervised spread, targeting only its intended destination. This indicates that while the system might be uncontrolled, its outputs were controllable[43]. Moreover, it illustrates that with proper programming and task stipulations, AWS could be utilized while adhering to fundamental principles.

Therefore, in determining whether an AWS should be inherently classified as indiscriminate, it is crucial to understand that nothing is inherent in the autonomy of the killing decision that would categorize these weapon systems as indiscriminate. Instead, this designation relies on different attributes of the system. Consequently, specific AWS could potentially be

40 Christopher Toscano, „«Friends of Humans», 189. P 208.

41 Jeffrey S. Thurnher, „Means and Methods of the Future: Autonomous Systems", [in:] *Targeting: the Challenges of Modern Warfare* (The Hague: TMC Asser Press, 2015), 186-187.

42 Ahmad Khalil, S. Anandha Krishna Raj, „Challenges to the Principle of Distinction in Cyber Warfare Navigating International Humanitarian Law Compliance" *Prawo i Więź* 49, No. 2 (2024): 109-131.

43 Dinniss Heather Harrison, *Cyber Warfare and the Laws of War* (Cambridge: Cambridge University Press, 2012) 255, n 41 159.

inherently indiscriminate; nevertheless, this trait will not be a common factor of the AWS as a category; thus, not all of them could be banned.

4.1.3. AWS and the Provision of „Legal Review of Weapons"

Article 36 of API establishes a crucial responsibility regarding weapons law under IHL. This obligation pertains to conducting a legal assessment of new weapons, methods, and means of warfare[44]. This assessment aims to ensure that the development, acquisition, or adoption of such weaponry aligns with the principles of IHL. Article 36 was introduced as a mechanism to tackle the challenges presented by technological advancements.

Reviewing AWS must consider the inherent features of these weapon systems. Conventional review procedures may prove insufficient in dealing with AWS owing the intricate nature and opacity of algorithms governing autonomy. Therefore, tailored measures, such as specialized software tools, have been proposed to verify the system's adherence to regulations and continuously evaluate testing and training performance[45]. While acknowledging that Article 36 reviews extend to AWS, it is essential to adapt these reviews to suit the specific characteristics of such systems.

Upon closer examination, Article 36 did not address the application of force against individuals. Rather, it mandates the establishment of national mechanisms that facilitate the testing of new weapons, following the rules and principles of IHL and other relevant international norms. Thus, when developing AWS, nations must guarantee that these emerging weapons adhere to the established regulations of weapons law, encompassing targeting law, and also comply with the rules and principles of the International Human Rights Law (IHRL) aimed at safeguarding the dignity and rights of individuals[46]. Crucially, Article 36 mandates that new weapons should be assessed against principles such as humanity. In addressing prohibitions and limitations grounded in customary and conventional weapons law, the ICRC's Guide finalizes with a brief section reserved for „Prohibitions or restrictions should adhere to principles of humanity and the dictates of public

44 Additional Protocol I (API) 1977 to the Geneva Conventions 1949.

45 Alec Tattersall, Damian Copeland, *Reviewing autonomous cyber capabilities* (2021), 205-257.

46 David A. Ruth, Paul Nielsen, „Defense Science Board Summer Study on Autonomy (Washington: Defense Technical Information Center, 2016).

conscience" – the Martens Clause[47]. As per the humanitarian establishment, the principle of humanity, as delineated in the Martens Clause, can be used to declare a weapon illegal. Hence, if (AWS) were judged to violate these „principles of humanity and dictates of public conscience", they would fail to meet the criteria of the legal review stipulated in Article 36 of API.

Nevertheless, the constraints and deficiencies arising from the review process are primarily contingent on how those assessments are carried out rather than on the specific technology being evaluated. In any case, AWS must undergo evaluation against the broader scope of IHL, encompassing regulations of weapons law, targeting law, and principles.

4.2. Targeting law

Moving to address the second aspect of regulations within IHL, which pertains to the appropriate use of force against individuals, known as targeting law. This body of regulation specifically deals with the lawful utilization of (legitimate) weapons in attacks. It emphasizes not the weapon itself but rather its wielder. Targeting law shares a common humanitarian principle with weapons law in that the parties involved in a conflict do not possess unlimited rights to attack each other. Therefore, it can be argued that both branches of IHL exhibit humanitarian characteristic as a fundamental feature. In this regard, we must initially refer to Article 48 of the API, that encloses the principle of distinction. According to this principle, parties engaged in a conflict must distinguish between protected individuals and combatants, as well as between civilian objects and military targets. It is mandatory to direct military operations against the latter only and is universally recognized as reflecting customary law, in particular, Rule 1[48].

The distinction between weapons law and targeting law centres on who is protected: while weapons law focuses on combatants, targeting law confirms that force is directed only towards acceptable targets, thus safeguarding civilians from injury. Targeting law standards foist the rights and obligations of parties involved in a conflict when preparing and executing an „attack". According to Article 49(1) of API, an „attack" refers to „acts

47 „A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977, January 2006" *IRRC*, No. 864 (2006): 933.

48 Customary International Humanitarian Law.

of violence against the adversary, whether in offense or defence". Hence, it is unanimous that AWS attacks fall under these norms. A vital issue to address is determining when an attack using AWS begins and its duration. One viewpoint suggests that an attack starts when the AWS select a target (narrow view). At the same time, another argues that it begins when AWS are activated (broad view). As the definition of „attack" affects the applicability of IHL rules, the latter view is preferable[49].

The current patterns observed at the CCW support the idea that humans and AWS will collaborate on the battlefield. Guiding Principle (c) acknowledges the crucial role of human-machine interaction, which can manifest in diverse ways and at different stages of the operational process. While a detailed discussion of this topic is beyond the scope of this discussion, it is important to note that these trends indicate that AWS, as a complete substitute for humans in combat, would be tricky. This underscores the significance of targeting law in evaluating whether such AWS can be utilized in compliance with IHL rules. Now, let us shift our focus to the primary norms within targeting law, which include the prohibition of indiscriminate attacks and the obligation to take precautions in an attack.

4.2.1 Deploying AWS and the Protection Against Indiscriminate Attacks

Derived from the principle of distinction, regulations against indiscriminate attacks establish a distinction between permitted and prohibited targets. The civilian population and individual civilians are not legitimate targets during conflicts. This prohibition, outlined in Article 51(2) of API and 13(2) of APII, is supplemented by more exhaustive rules constraining parties involved in a conflict.

Moreover, it is important to emphasize that the prohibition of indiscriminate attacks is of great importance within the framework of the targeting law. The most important rules consistent with the context of AWS deployment fall into two categories. First, the principle of discrimination contains many rules that are important in classifying individuals when launching an attack, those whose targeting is legal and those whose

49 Vincent Boulanin, Neil Davison, Netta Goussac, Moa Peldán Carlsson, *Limits on Autonomy in Weapon Systems: Identifying Practical elements of Human Control* (2020).

targeting is illegal. Second, proportionality is a principle that balances expected and actual military advantages and reduces collateral damage.

4.2.1.1. AWS AND THE PRINCIPLE OF DISTINCTION

First, the rule against indiscriminate attacks mandates that the involved party in a conflict abstain from employing tactics that lack discrimination. These tactics encompass warfare methods aimed at protecting individuals or objects, thereby starkly contravening the standards mentioned earlier. This rule is succinctly articulated in Article 51(4)(a) of the API, which explicitly prohibits indiscriminate attacks as those not aimed at a distinct military target, a rule widely recognized as customary.

This rule complements the one against indiscriminate weapons, concurrently, they constitute a set of rules representing the core principle of distinction outlined in Article 48 of API. According to this fundamental rule, parties engaged in a conflict must always distinguish between civilians and combatants, as well as between civilian objects and military targets, leading their actions solely towards the latter. Articles 51(2) and 52(1) elaborate on this principle.

The primary challenge faced by a commander when opting to deploy AWS are ensuring that attacks conducted through them are aimed solely at legitimate targets. A key concern commonly linked with remote warfare is that the likelihood of misidentifying targets escalates due to the separation of humans from the battlefield and the reliance on automated or autonomous systems for crucial functions[50]. To mitigate and eliminate these risks, AWS must be able to assess the status of individual targets before initiating engagement. However, depending on the circumstances, an autonomous system may have difficulty making such assessments accurately.

According to Article 52(2) of API, the classification of „military objectives" encompasses „objects that, due to their nature, location, purpose, or utility, contribute significantly to military activities, and whose complete or partial destruction, capture, or neutralization, in the prevailing circumstances, provides a clear military advantage"[51].

---

50 Emily Crawford, „The Principle of Distinction and Remote Warfare", [in:] *Research Handbook on Remote Warfare* (Cheltenham: Edward Elgar Publishing, 2017), 50-78.

51 Horace B. Robertson, „The Principle of the Military Objective in the Law of Armed Conflict", [in:] *The Development and Principles of International Humanitarian Law* (London: Routledge, 2017), 531-557.

Although identifying a military target based on its „essence" might appear straightforward, AWS will require qualified sensors to distinguish a military vehicle from a civilian one[52]. Parameters such as „purpose" or „emploi" pose greater challenges for assessment, inevitably necessitating a context-dependent evaluation. The ICRC's Commentary describes the notion of „purpose" as the planned utilization of an object, while the notion of „use" pertains to its current role. It must be pointed out that the concept of concrete military advantage has been subject to many interpretations, but raising such an issue results in a loss of protection for civilians and civilian objects[53].

To comply with these rules, AWS must have algorithms that can process vast amounts of time-sensitive data. In addition, determining the military value of a target requires an assessment of the immediate military advantage to be gained from an attack, which is another challenge for algorithms[54]. Consequently, some suggest deploying AWS solely in structured, simplified environments, where algorithms can reliably make exact time assessments[55]. In international armed conflicts (IAC), identifying combatants on the battlefield can be challenging because IHL does not mandate a specific uniform for regular forces, only requiring irregular forces to carry their weapons openly.

It is important to navigate the extent of human control required over AWS in adhering to the rule against indiscriminate attacks, particularly when these machines undertake crucial roles on the battlefield. A common argument questions the compatibility of AWS with targeting laws, suggesting that the subjective and context-dependent nature of categorizing individuals clashes with algorithmic systems, making it challenging to employ AWS in an IHL-compliant manner. However, this argument presents a technological constraint against AWS, which may change with future advancements. For instance, developments in deep-learning algorithms could enable AWS to differentiate between permissible and non-permissible

52 Markus Wagner, „Autonomy in the Battlespace: Independently Operating Weapon Systems and the Law of Armed Conflict", [in:] *International Humanitarian Law and the Changing Technology of War* (Leiden: Brill Nijhoff, 2013), 99-122.

53 Michael N. Schmitt, „Targeting and Humanitarian Law: Current Issues" *Israel Yearbook on Human Rights*, Vol. XXXIV (2004): 59-104.

54 Wagner, „Autonomy in the battlespace", 99-122.

55 Matthias Brenneke, „Lethal Autonomous Weapon Systems and their Compatibility with International Humanitarian Law: a Primer on the Debate" *Yearbook of International Humanitarian Law*, Vol. XXI (2020): 59-98.

targets. Therefore, if algorithmic systems can ensure the proper categorization of individuals, it implies compliance with rules against indiscriminate attacks. The recent United Nations General Assembly Resolution on AI assured this. Although the resolution is not aimed at the military sector, it confirms that the development of reliable AI should keep pace with the urgent need to reach a global consensus on safe, secure, and trustworthy AI systems[56].

In combat situations, one of the challenges for AWS will be identifying when a combatant surrenders and thus gain protected status. Once surrendered, the individual cannot be targeted. AWS must be equipped to recognize and acknowledge surrender, requiring suitable sensors and algorithms to accurately detect and interpret human behavior. While some authors have highlighted the technological difficulties in these situations, this does not warrant a complete ban on AWS[57].

While it is plausible to argue that AWS do not violate the rule against indiscriminate attacks when human operators are not directly involved in target selection and engagement, the crucial aspect is determining the level of „human control" required over vital functions. At its core, AWS must be able to „classify" targets to ensure proper discrimination. While autonomous systems excel in „observing" and „recognizing" potential targets, the decision to use lethal force is more uncertain and may necessitate human intervention. Therefore, human operators may retain control to intervene, when necessary, especially in situations where categorizing a specific individual is uncertain.

In situations of uncertainty regarding status, targeting law mandates parties to a conflict to assume that the individual is civilian. This principle aligns with customary law, emphasizing the need to refrain from automatically attacking anyone who appears dubious. Applied to AWS, this principle prohibits autonomous systems from attacking when there is doubt about an individual's status. In such cases, human operators are required to intervene. However, humans do not need to intervene every time doubt arises regarding the permissibility of a target. This may be suitable initially, but as autonomous systems become more advanced, they may handle doubt effectively. For instance, it is suggested that AWS should convert doubts into a measurable probability, classifying individuals below a certain threshold

56 UN General Assembly resolution on AI, document A/78/L.49, 21 March 2024.

57 Robert Sparrow, „Twenty Seconds to Comply: Autonomous Weapon Systems and the Recognition of Surrender" *International Law Studies*, No. 1 (2015): 20.

as civilians[58]. If the AWS operate comparably to a reasonable human in the same situation, they comply with the doubtful rule.

The conclusion we arrived at can be summarized that, the absence of human intervention in target selection and engagement does not inherently violate the principles of distinction, provided that AI techniques integrated into AWS enable accurate categorization of human targets.

4.2.1.2 AWS AND THE RULES OF THE PRINCIPLE OF PROPORTIONALITY

Another set of rules that require human oversight of AWS is derived from the principle of proportionality. The prohibition against direct attacks on civilians does not mean that civilians cannot be targeted under any circumstances. The principle of proportionality states that when strategizing and conducting an attack, the anticipated military advantages must be weighed against the expected civilian harm, often known as „collateral damage". Essentially, civilian harm is not automatically forbidden; it only becomes unacceptable when disproportionate[59].

This introduces an additional level of notional complexity: not only will parties engaged in a conflict need to utilize methods and strategies to classify targets accurately, but they will also have to evaluate the potential military advantages of executing a specific attack and compare it with the anticipated collateral damage. Nevertheless, in warfare, collateral damage is inevitable; it is impossible to envision warfare without it[60].

Article 51(5)(b) states that an attack is considered „indiscriminate" when the unintended harm to civilians or their objects exceeds the anticipated military advantage. If this occurs, according to Article 57(2)(b), the attack must be halted or aborted. While such rules are not explicitly stated in the APII, they are generally accepted as applicable to non-international armed conflicts (NIAC) on the basis of humanitarian principles or as custom.

At the functioning stage, achieving equilibrium consisting of the principle of proportionality entails a thorough three-phase analysis beforehand: (1) estimating potential collateral damage, (2) evaluating military

58 Joshua G. Hughes, „The Law of Armed Conflict Issues Created by Programming Automatic Target Recognition Systems Using Deep Learning Methods" *Yearbook of International Humanitarian Law*, Vol. XXI (2018): 99-135.

59 Gregor Noll, „Analogy at War: Proportionality, Equality and the Law of Targeting" *Netherlands Yearbook of International Law*, 43 (2012): 205-230.

60 Yoram Dinstein, *Discussion: Reasonable Military Commanders and Reasonable Civilians. Legal and Ethical Lessons of NATO's Kosovo Campaign* (Newport: Naval War College, 2002).

advantages, and (3) discerning any excessiveness[61]. In the initial step, proportionality mandates assigning significance to the expected collateral damage, which varies depending on the characteristics of the target, for instance, the presence of vulnerable individuals and the severity of the harm, where injuries are typically considered less severe than loss of life.

In assessing military advantages, a major concern centers on the complex issue of self-protection, which is especially pertinent to AWS. A scenario where no personnel are harmed in an attack, such as the matter with an AWS, appears inherently advantageous from a military standpoint. However, suggesting that an attacker with superior weaponry can obliterate the enemy and view civilian casualties as collateral damage is morally repugnant. To prevent such a scenario, it is strongly recommended that the safety of the attacking forces not be factored into the calculation of the military advantage.

The final phase, assessing excessiveness, stands out as particularly intriguing. Proportionality-based regulations necessitate balancing conflicting weights: military advantage and collateral damage. There is been speculation about whether these capabilities could be translated into algorithms and, more broadly, whether the assessment of proportionality could be delegated entirely to AWS[62].

Matching these interests poses a challenging duty for humans themselves. Balancing involves naturally unique and context-dependent evaluations based on reasonableness and excessiveness, which adhere to a standard akin to a well-informed individual[63]. However, this does not imply that such standards are arbitrary, as they are ultimately based on the beliefs and knowledge of the agent involved.

Due to the complexity of this equilibrium, it is argued that algorithmic techniques are structurally insufficient to meet that criterion[64]. Accordingly, some propose a ban on AWS, while others suggest that AWS can adhere to proportionality rules with proper adjustments in human supervision[65]. Major military powers globally have funded AI systems capable of estimating collateral damage using matter-of-fact norms, which

61 Petra Rešlová, *Meaningful Human Control in Autonomous Weapons* (2023).

62 Jeroen Van Den Boogaard, „Proportionality and Autonomous Weapons Systems" *Journal of International Humanitarian Legal Studies*, No. 2 (2015): 247-283.

63 Enzo Cannizzaro, *Proportionality in the Law of Armed Conflict* (2014).

64 Michael N. Schmitt, „Autonomous Weapon Systems and International Humanitarian Law: a Reply to the Critics" *Harvard National Security Journal Feature* (2012).

65 Supra not (6).

can be rephrased as algorithmic vocabulary[66]. Nevertheless, these systems have been criticized for not being able to translate moral considerations into algorithmic codes, such as feelings and reason.

If the result is reasonably consistent with a conjectural human agent, full compliance with the relevant rules is achieved. Furthermore, in IHL, the benchmark ensuring reasonableness through the ability to understand and justify the actions of AWS, which is crucial[67]. It is essential to recognize that proportionality rules present challenging missions to military personnel, requiring them to balance military necessities with human values. This complexity makes it inappropriate to embody proportionality rules in the algorithms. However, it is important to note that future advancements may lead to the development and deployment of AWS that operate in accordance with proportionality constraints.

4.2.2. AWS and the Precautionary Principle

The stipulation embedding the obligation to exercise precaution in attacks, as outlined in Article 57 of the API, commences with a fundamental principle mandating the application of „continuous supervision" in safeguarding civilians and civilian objects. The term „continuous" implies an enduring commitment, and the expansive interpretation of „military proces" reaffirms that this obligation remains incumbent upon parties involved in a conflict throughout its duration. Regarding restrictions concerning indiscriminate attacks, precautionary measures also hinge upon contextual evaluations and are aligned with a measure of properness.

Additionally, there exist regulations mandating the selection of means and methods of warfare aimed at mitigating or averting collateral damage, alongside the choosing of targets anticipated to pose the least risk of collateral harm. Furthermore, precautionary principles necessitate parties to a conflict to abstain from initiating attacks and to halt or annul ongoing attacks when it becomes evident that they cannot adhere to the principles of distinction and proportionality. Finally, when attacks are anticipated

66 Jeffrey S. Thurnher, „Feasible Precautions in Attack and Autonomous Weapons", [in:] *Dehumanization of Warfare: Legal Implications of New Weapon Technologies* (Berlin-Heidelberg: Springer Verlag, 2018), 99-117.

67 Michael N. Schmitt, Jeffrey S. Thurnher, „Out of the Loop: Autonomous Weapon Systems and the Law of Armed Conflict" *Harvard National Security Journal*, 4 (2012): 231.

to impact the civilian populace, parties must provide „effective warning" whenever feasible to reduce civilians' openness to preventable harm.

Taken collectively, these rules operationalize most laws pertaining to weapons and targeting, as discussed earlier. The utilization of AWS in armed conflicts is anticipated to pose significant challenges for parties opting to employ them. Miscellaneous suggestions have been made concerning executing precautionary measures when specific crucial functions are delegated to unsupervised autonomous systems operating. To achieve the precautions' objective, it is imperative that human operators consistently observe and deactivate any AWS instances that exhibit unauthorized behaviour[68]. Leaving a „kill buton" for AWS, a fail-safe measure against clear violations of admissible conduct by AWS, presents developers with technological hurdles, such as mitigating threats of spoofing or hacking. Nevertheless, maintaining human oversight in line with the fundamental precautionary principle remains critical[69].

A perspective has been put forward likening AWS to „fire-and-forget" projectiles, which cannot be recalled once launched and do not raise concerns about compatibility with IHL if human operators cannot recall them post-deployment. However, this conceit's applicability for AWS depends heavily on the operational environment and the system's intended targets. While it may hold in military settings, environments with civilian presence may necessitate human intervention, possibly by an override mechanism or operator regular check-in[70]. Given these characteristics, it is evident that adherence to precautionary measures in targeting mandates a level of human control over AWS to make instructed decisions on their deployment. Commanders must comprehend the capacities of AWS in a given context and take necessary precautions[71].

Nevertheless, systems that facilitate improved collaboration between humans and machines may prove pivotal. Therefore, the opinion that some decisions regarding target selection and engagement could be made

68 Kjølv Egeland, „Lethal Autonomous Weapon Systems Under International Humanitarian Law" *Nordic Journal of International Law*, No. 2 (2016): 89-118.

69 Henderson, Keane, Liddy, „Remote and Autonomous Warfare Systems", 335-370.

70 Maziar Homayounnejad, „Ensuring Fully Autonomous Weapons Systems Comply with the Rule of Distinction in Attack", [in:] *Drones and Other Unmanned Weapons Systems under International Law* (Leiden: Brill Nijhoff, 2018), 123-157.

71 Marco Sassoli, „Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified" *International Law Studies*, No. 1 (2014): 1.

unsupervised humans is not vigorous; precautionary actions can be established to meet IHL requirements regardless of human intervention in crucial decision-making processes.

4.2.3. The Marten's Clause: A Controversial Perspective on AWS

The assessment of emerging technology by the principle of humanity within the framework of IHL incontrovertibly carries influential weight. The legal importance, or authoritative mandate, of this principle is broadly discussed in IHL circles owing to its notional conjectural nature and functional ramifications. It is pleaded that the Martens Clause in IHL operates akin to Article 38 of the Statute of the ICJ, which delineates the origins of the legal framework[72]. Nevertheless, a constant controversy exists concerning the legal potency of the principle of humanity, as mentioned in the Martens Clause, from different doctrinal and jurisprudential viewpoints.

Some argue that the principle of humanity lacks autonomous, legally binding effects and cannot prohibit specific weapons or methods of warfare on its own. This view is supported by the observation that no weapon has been declared illegal based solely on the Martens Clause[73]. Instead, domestic and international case law tend to use the clause to confirm existing legal solutions, offer new interpretations, or reject arguments. However, this stance risks rendering the clause redundant, merely reiterating existing norms. While the clause explicitly refers to established custom[74], its mention of „principles of humanity and dictates of public conscience" suggests consideration of other sources of law, prompting alternative interpretations. Another group of interpreters contends that the Martens Clause influences the sources of international law, with some advocating a more significant role for natural law[75]. They argue that the clause operates beyond positive law, embodying moral imperatives with

72 Jeroen C. van den Boogaard, „Fighting by the Principles: Principles as a Aource of International Humanitarian Law", [in:] Mariëlle Matthee, Brigit Toebes, Marcel Bru, *Armed Conflict and International Law: In Search of the Human Face: Liber Amicorum in Memory of Avril McDonald* (The Hague: Springer, 2013), 3-31.

73 Elena Carpanelli, „General Principles of International Law: Struggling with a Slippery Concept", [in:] *General Principles of Law-The Role of the Judiciary* (Cham: Springer International Publishing, 2015), 125-143.

74 Georges Abi-Saab, *The Specificities of Humanitarian Law* (1984).

75 Antonio Cassese, „The Martens Clause: Half a Loaf or Simply Pie in the Sky?", [in:] *The Development and Principles of International Humanitarian Law* (London: Routledge, 2017), 373-402.

a binding force. Some ICJ judges have implicitly or explicitly invoked extra-positive law to support their positions. This perspective underscores the close connection between IHL and extra-positive values[76].

However, questions remain about the inconsistent binding effect of legal sources, such as the principle of humanity. It remains uncertain whether the principle should be considered a binding source, without a middle ground. Transitioning to the specific realm of AWS, the principle of humanity assumes heightened significance. As technological advancements reshape the nature of warfare, ethical considerations surrounding the deployment of autonomous systems have become increasingly prominent. The Martens Clause, with its emphasis on humanitarian values, provides a framework for evaluating AWS deployment's ethical and legal implications.

Due to its compelling moral foundation, the principle of humanity is a significant argument for NGOs that oppose AWS[77]. Human Rights Watch, for instance, frequently cites this principle in its reports, using it as a basis to challenge the legality of AWS. While there is no unanimous agreement among experts and the general public regarding the acceptability of autonomous killing, a considerable number find the concept deeply troubling and unacceptable. States are urged to consider these perspectives when assessing dictates of public conscience.

The ICRC also emphasizes the significance of the „principles of humanity" and „dictates of public conscience", viewing them as inherently linked to morality and distinct from positive law[78]. However, the ICRC does not offer clear arguments regarding the normative status of these principles. Nonetheless, AWS raise ethical concerns that require translation into legal terms; failure to do so could imply permissibility under IHL[79]. Some authors advocate for a normative role for the principle of humanity, arguing that discussions on legal and moral standards for killing cannot

76 Hilly Moodrick-Even Khen, „Aidōs and Dikē in International Humanitarian Law: Is IHL a Legal or a Moral System?" *The Monist*, No. 1 (2016): 26-39.

77 Amanda Sharkey, „Autonomous Weapons Systems, Killer Robots and Human Dignity" *Ethics and Information Technology*, No. 2 (2019): 75-87.

78 Jérémie Labbé, Pascal Daudin, „Applying the Humanitarian Principles: Reflecting on the Experience of the International Committee of the Red Cros" *International Review of the Red Cross*, No. 897-898 (2015): 183-210.

79 Schmitt, Thurnher, „Out of the Loop", 231.

overlook essential human qualities, such as conscience, common sense, and intuition, which cannot be programmed into machines[80].

In this context, the principle of humanity requires careful consideration of the potential humanitarian consequences of autonomous weapons. It advocates a balanced approach that considers military necessity and ethical concerns. This underscores the imperative for human responsibility in decision-making processes, ensuring accountability and compliance with fundamental principles of humanity and the dictates of public conscience.

In essence, general principles similar to those in IHRL can be identified in IHL. Humanity, as a core value, can be regarded as a general principle of IHL, allowing for its application in cases where existing IHL rules, such as AWS, may fall short.

By integrating the principle of humanity into discussions on AWS, policymakers, and legal experts can navigate the intricate ethical and legal challenges posed by emerging technologies. This approach ensures that advancements in warfare remain aligned with the overarching goal of preserving human dignity and minimizing the cost of armed conflict, following established international legal principles and humanitarianism.

In summary, the principle of humanity provides a strong legal foundation for asserting that delegating critical functions to machines, with human operators having minimal to no power to intervene, is unacceptable. However, state and non-state actors often invoke the Martens Clause more as a tool to influence future lawmaking than as a strictly legal imperative. While some view it primarily as a moral guideline, others seek to ensure that the development and deployment of AWS align with IHL rules. In cases where „human control" is maintained, and human operators can understand and explain the actions of AWS in compliance with IHL, the use of AWS are deemed permissible. However, in both scenarios, the significance of the principle of human dignity was greatly underestimated.

80 Mary Ellen O'Connell, „Banning Autonomous Killing: The Legal and Ethical Requirement that Humans Make Near-time Lethal Decisions", [in:] *The American Way of Bombing: How Legal and Ethical Norms Change* (Cornell: Cornell university Press, 2014): 224-236.

5 Conclusion

The evolving landscape of warfare, driven by new tactics, geopolitical shifts, and technological advances, necessitates a legal debate to regulate emerging combat technologies, such as AWS. The concept of autonomy in weapon systems further complicates the debate, with definitions and distinctions between automatic and autonomous systems remaining ambiguous. The development of AWS is progressing globally, with various countries investing in advanced systems for military applications. The capacity of technology to detect human emotions raises additional legal and ethical concerns, yet some argue that appropriate control procedures can ensure AWS compliance with international law. Given these complexities, a comprehensive legal analysis of AWS from the perspective of weapons law and targeting law is necessary to navigate the ethical and legal implications effectively. Such an analysis will contribute to shaping responsible governance frameworks and ensuring the adherence of AWS to international humanitarian principles.

The legal examination of the development and use of AWS has revealed the complexity of evaluating these technologies under IHL. Two aspects have been studied to assess legality of AWS: weapons law and targeting law. Weapons' law, governed by the IHL, evaluates weapons' lawfulness and inherent characteristics. Article 35 of the API prohibits weapons from causing superfluous injury or unnecessary suffering, establishing the legality criteria for AWS. Although AWS's autonomy introduces complexity, it does not inherently render them unlawful, because their impact depends on specific scenarios and programming.

Regarding the targeting law, the AWS must distinguish between military objectives and civilian targets, as mandated by Article 51(4)(b) of the API. Current technological limitations may challenge AWS's ability to distinguish themselves effectively in certain scenarios, but potential advancements could improve their capability. Additionally, AWS must undergo a legal review process, as outlined in Article 36 of API, to ensure compliance with IHL principles, including humanity.

While challenges exist in evaluating AWS's adherence to IHL, tailored review processes and continuous assessments can help address these complexities.

The principle of humanity, enshrined in the Martens Clause, plays a pivotal role in evaluating the ethical and legal implications of deploying AWS within the framework of IHL. While the Martens Clause is often invoked

more as a tool to influence future law-making than as a strict legal imperative, it underscores the imperative for human responsibility in decision-making processes regarding AWS.

Consequently, AWS must adhere to IHL rules, with human control maintained to intervene when necessary, and operators must be able to understand and explain AWS actions in compliance with IHL. However, regardless of the specific legal interpretations and applications, the significance of upholding human dignity remains paramount in discussions surrounding the development and deployment of AWS.

Finally, it is mandatory to Promote Transparency and Accountability; mechanisms for transparency and accountability must be established to ensure that the use of AWS is conducted responsibly and ethically. This includes robust monitoring, reporting, review processes, and mechanisms for addressing violations of IHL and ethical standards.

Bibliography

A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977, January 2006" *IRRC*, No. 864 (2006).

Abi-Saab Georges, *The Specificities of Humanitarian Law* (1984).

Anderson Kenneth, Reisner Daniel, Waxman Matthew C., „Adapting the Law of Armed Conflict to Autonomous Weapon Systems" *International Law Studies*, (2014): 386-411.

Asaro Peter, „Jus Nascendi. Robotic Weapons and the Martens Clause", [in:] *Robot Law*, ed. Michael A. Froomkin, Ryan Calo, Ian Kerr, Edward Elgar. 367-386. Cheltenham, 2016. https://doi.org/10.4337/9781783476732.00024.

Azaria Asaph, Asma Ghandeharioun, Akane Sano, Rosalind Picard, Natasha Jaques, Sara Taylor, *Predicting Students' Happiness from Physiology, Phone, Mobility, and Behavioral Data*. International Conference on Affective Computing and Intelligent Interaction and workshops: [proceedings]. ACII (Conference), September 2015. https://pubmed.ncbi.nlm.nih.gov/28515966/.

Bitar Mohammad Chakka Benarji, „Drone Attacks During Armed Conflict: Quest for Legality and Regulation" *International Journal of Intellectual Property Management*, No. ¾ (2023): 97-411.

Boulanin Vincent, Neil Davison, Netta Goussac, Moa Peldán Carlsson, *Limits on Autonomy in Weapon Systems: Identifying Practical elements of Human Control*. 2020.

Brenneke Matthias, „Lethal Autonomous Weapon Systems and their Compatibility with International Humanitarian Law: a Primer on the Debate" *Yearbook of International Humanitarian Law*, Vol. XXI (2020): 59-98.

Cannizzaro Enzo, *Proportionality in the Law of Armed Conflict*. 2014.

Carpanelli Elena, „General Principles of International Law: Struggling with a Slippery Concept", [in:] *General Principles of Law-The Role of the Judiciary*. 125-143. Cham: Springer International Publishing, 2015.

Cassese Antonio, The Martens Clause: Half a Loaf or Simply Pie in the Sky?", [in:] *The Development and Principles of International Humanitarian Law*. 373-402. London: Routledge, 2017.

Choi Charles Q., Mood-Detecting Sensor Could Help Machines Respond to Emotions" *IEEE Spectrum*, 24 June 24 2021. https://spectrum.ieee.org/mooddetecting-sensor-could-help-machines-respond-to-emotions.

Coker Christopher, „On Banning Autonomous Weapon Systems: Human Rights, Automation and the Dehumanization of Lethal Decision Making" *Future Wars*, (2015): 57-60.

Coupland Robin M., Review of the Legality of Weapons: a New Approach" International Review of the Red Cross, No. 835 (1999): 583-592.

Crawford Emily, „The Principle of Distinction and Remote Warfare", [in:] *Research Handbook on Remote* Warfare. 50-78. Cheltenham: Edward Elgar Publishing, 2017.

Crootof Rebecca, „The Killer Robots Are Here: Legal and Policy Implications" *Cardozo Law Review*, No. 5 (2015): 1837-1916.

Dinniss Heather Harrison, *Cyber Warfare and the Laws of War*. Cambridge: Cambridge University Press, 2012.

Dinstein Yoram, *Discussion: Reasonable Military Commanders and Reasonable Civilians. Legal and Ethical Lessons of NATO's Kosovo Campaign*. Newport: Naval War College, 2002.

Drew James, „USAF's Small UAS Roadmap Calls for Swarming «kamikaze» Drones" *Flight Global*, 10 December 2019. https://www.flightglobal.com/civil-uavs/usafs-small-uas-roadmap-calls-for-swarming-kamikaze-drones/120493.article.

Egeland Kjølv, „Lethal Autonomous Weapon Systems Under International Humanitarian Law" *Nordic Journal of International Law*, No. 2 (2016): 89-118.

Expert Meeting: Autonomous Weapon System: Technological, Military, Legal, and Humanitarian Aspects" *ICRC*, (2014).

Ford Christopher M., Autonomous Weapons and International Law" *South Carolina Law Review*, 69 (2017): 413-478.

Forestier-Walker Robin, „Nagorno-Karabakh: New Weapons for an Old Conflict Spell Danger" *Al Jazeera*, 13 October 2020. https://www.aljazeera.com/features/2020/10/13/nagorno-karabakh-new-weapons-for-an-old-conflict-spell-danger.

Haight Joel M., Vladislav Kecojevic, „Automation vs. human intervention: What is the best fit for the best performance?" *Process Safety Progress*, No. 1 (2005): 45-51.

Handy Brian, *Royal Air Force Aircraft & Weapons (DCC(RAF)*. Publications Belmont Press, 2007.

Hardy Michael, „Pentagon Proves Air-Launched UAV Swarm Ability" *C4ISRNet*, 19 August 2022. https://www.c4isrnet.com/unmanned/uas/2016/03/15/pentagon-proves-air-launched-uav-swarm-ability/.

Hayir Nurbanu, „Defining Weapon Systems with Autonomy: The Critical Functions in Theory and Practice" *Groningen Journal of International Law*, No. 2 (2022): 239-265.

Henderson Ian, Patrick Keane, Joshua Liddy, „Remote and Autonomous Warfare Systems – Precautions in Attack and Individual Accountability", [in:] *Research Handbook on Remote Warfare*, ed. Jens David Ohlin. Cheltenham: Edward Elgar Press, 2016.

Hernandez Joe, „A Military Drone with a Mind of Its Own Was Used in Combat, U.N. Says" *NPR*, 1 June 2021. https://www.npr.org/2021/06/01/1002196245/a-u-n-report-suggests-libya-saw-the-first-battlefield-killing-by-an-autonomous-d.

Heyns Christof, „Extrajudicial, Summary or Arbitrary Executions" *Security Issues in the Greater Middle East*, (2013).

Homayounnejad Maziar, „Ensuring Fully Autonomous Weapons Systems Comply with the Rule of Distinction in Attack", [in:] *Drones and Other Unmanned Weapons Systems under International Law*. 123-157. Leiden: Brill Nijhoff, 2018.

Hughes Joshua G., „The Law of Armed Conflict Issues Created by Programming Automatic Target Recognition Systems Using Deep Learning Methods" *Yearbook of International Humanitarian Law*, Vol. XXI (2018): 99-135.

Khalil Ahmad, S. Anandha Krishna Raj, „Challenges to the Principle of Distinction in Cyber Warfare Navigating International Humanitarian Law Compliance" *Prawo i Więź* (2024).

Khen Hilly Moodrick-Even, „Aidōs and Dikē in International Humanitarian Law: Is IHL a Legal or a Moral System?" *The Monist*, No. 1 (2016): 26-39.

Labbé Jérémie, Pascal Daudin, „Applying the Humanitarian Principles: Reflecting on the Experience of the International Committee of the Red Cros" *International Review of the Red Cross*, No. 897-898 (2015): 183-210.

Lewis Dustin A., „Three Pathways to Secure Greater Respect for International Law Concerning War Algorithms" *Harvard Law School.PILAC* (2020). https://pilac.law.harvard.edu/three-pathways-to-secure-greater-respect-for-international-law-concerning-war-algorithms.

Lucas Jr George R., „Automated Warfare" *Stanford Law & Policy Review*, 25 (2014): 317-340.

McDuff Daniel J., Javier Hernandez, Sarah Gontarek, Rosalind W. Picard, „Cogcam" *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, No. 3 (2016): 4000–4004. https://doi.org/10.1145/2858036.2858247.

Melzer Nils, *Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare*. Directorate-General for External Policies, European Parliament, 2013.

Morillo Stephen, *What is Military History?*. Hoboken: John Wiley & Sons, 2017.

„Neuron Unmanned Combat Air Vehicle (UCAV) Demonstrator" *Airforce Technology*, 18 February 2020. https://www.airforce-technology.com/projects/neuron/.

Noll Gregor, „Analogy at War: Proportionality, Equality and the Law of Targeting" *Netherlands Yearbook of International Law*, 43 (2012): 205-230.

O'Connell Mary Ellen, „Banning Autonomous Killing: The Legal and Ethical Requirement that Humans Make Near-time Lethal Decisions", [in:] *The American Way of Bombing: How Legal and Ethical Norms Change*. 224-236. Cornell: Cornell University Press, 2014.

Reeves Shane, William Johnson, „Autonomous Weapons: Are You Sure These Are Killer Robots? Can We Talk About It?" *The Army Lawyer*, (2014).

Rešlová Petra, *Meaningful Human Control in Autonomous Weapons* (2023).

Robertson Horace B., „The Principle of the Military Objective in the Law of Armed Conflict", [in:] *The Development and Principles of International Humanitarian Law*. 531-557. London: Routledge, 2017.

Ruth A. David, Paul Nielsen, „Defense Science Board Summer Study on Autonomy. Washington: Defense Technical Information Center, 2016.

Sassoli Marco, „Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified" *International Law Studies*, No. 1 (2014): 308-340.

Scharre Paul, Michael C. Horowitz, „Autonomy in Weapon Systems" *Center for a New American Security Working Paper*, (2015).

Schmitt Michael N., „Autonomous Weapon Systems and International Humanitarian Law: a Reply to the Critics" *Harvard National Security Journal Feature* (2012).

Schmitt Michael N., „Out of the Loop: Autonomous Weapon Systems and the Law of Armed Conflict" *Harvard National Security Journal*, 4 (2012): 321-

Schmitt Michael N., „Targeting and Humanitarian Law: Current Issues" *Israel Yearbook on Human Rights*, Vol. XXXIV (2004): 59-104.

Sharkey Amanda, „Autonomous Weapons Systems, Killer Robots and Human Dignity" *Ethics and Information Technology*, No. 2 (2019): 75-87.

Sparrow Robert, Twenty Seconds to Comply: Autonomous Weapon Systems and the Recognition of Surrender" *International Law Studies*, No. 1 (2015): 699-728.

„STM Kargu" *Smartencyclopedia*, 4 January 2023. https://smartencyclopedia.org/content/stm-kargu/.

Suchman Lucy, „Algorithmic Warfare and the Reinvention of Accuracy" *Critical Studies on Security*, No. 2 (2020): 175-187. https://doi.org/10.1080/21624887.2020.1760587.

Surabhi Ankita, *From „Killer Robots" to Autonomous Weapons Systems (AWS)*, 2019.

Taddeo Mariarosaria, Alexander Blanchard, „A Comparative Analysis of the Definitions of Autonomous Weapons", [in:] *The 2022 Yearbook of the Digital Governance Research Group*. 57-79. Cham: Springer Nature Switzerland, 2023.

Tattersall Alec, Damian Copeland, *Reviewing autonomous cyber capabilities*. 2021.

Thurnher Jeffrey S., „Means and Methods of the Future: Autonomous Systems", [in:] *Targeting: the Challenges of Modern Warfare*. 186-187. The Hague: TMC Asser Press, 2015.

Thurnher Jeffrey S., Feasible Precautions in Attack and Autonomous Weapons", [in:] *Dehumanization of Warfare: Legal Implications of New Weapon Technologies*. 99-117. Berlin-Heidelberg: Springer Verlag, 2018.

Toscano Christopher, „«Friends of Humans»: An Argument for Developing Autonomous Weapons Systems" *Journal of National Security Law & Policy*, No. 1 (2015): 189-246.

Turns David, „Weapons in the ICRC Study on Customary International Humanitarian Law" *Journal of Conflict & Security Law*, No. 2 (2006): 201-237.

Van Den Boogaard Jeroen, „Proportionality and Autonomous Weapons Systems" *Journal of International Humanitarian Legal Studies*, No. 2 (2015): 247-283.

Van Den Boogaard, Jeroen C., „Fighting by the Principles: Principles as a Aource of International Humanitarian Law", [w:] Mariëlle Matthee, Brigit Toebes, Marcel Bru, *Armed Conflict and International Law: In Search of the Human Face: Liber Amicorum in Memory of Avril McDonald*. 3-31. The Hague: Springer, 2013.

Wagner Markus, „Autonomy in the Battlespace: Independently Operating Weapon Systems and the Law of Armed Conflict", [in:] *International Humanitarian Law and the Changing Technology of War*. 99-122. Leiden: Brill Nijhoff, 2013.

Weber Jutta, Lucy Suchman, „Human–Machine Autonomies", [in:] *Autonomous Weapons Systems: Law, Ethics, Policy*, ed. Nehal Bhuta, Susanne Beck, Robin Geiβ, Hin-Yan Liu, Claus Kreβ. 75-102. Cambridge: Cambridge University Press, 2016.

Yan Liu Hin, „Categorization and Legality of Autonomous and Remote Weapons Systems" *International Review of the Red Cross*, No. 886 (2012).

Zajac Maciej, „Beyond Deadlock: Low Hanging Fruit and Strict yet Achievable Options in AWS Regulation" *Journal of Ethics and Emerging Technologies*, No. 2 (2022): 1-14.